MyData and the Identity Conundrum

(or, "How you can stop worrying and learn to love NSTIC")

Jeremy Grant

Senior Executive Advisor, Identity Management

National Institute of Standards and Technology (NIST)

Sharing data is good.

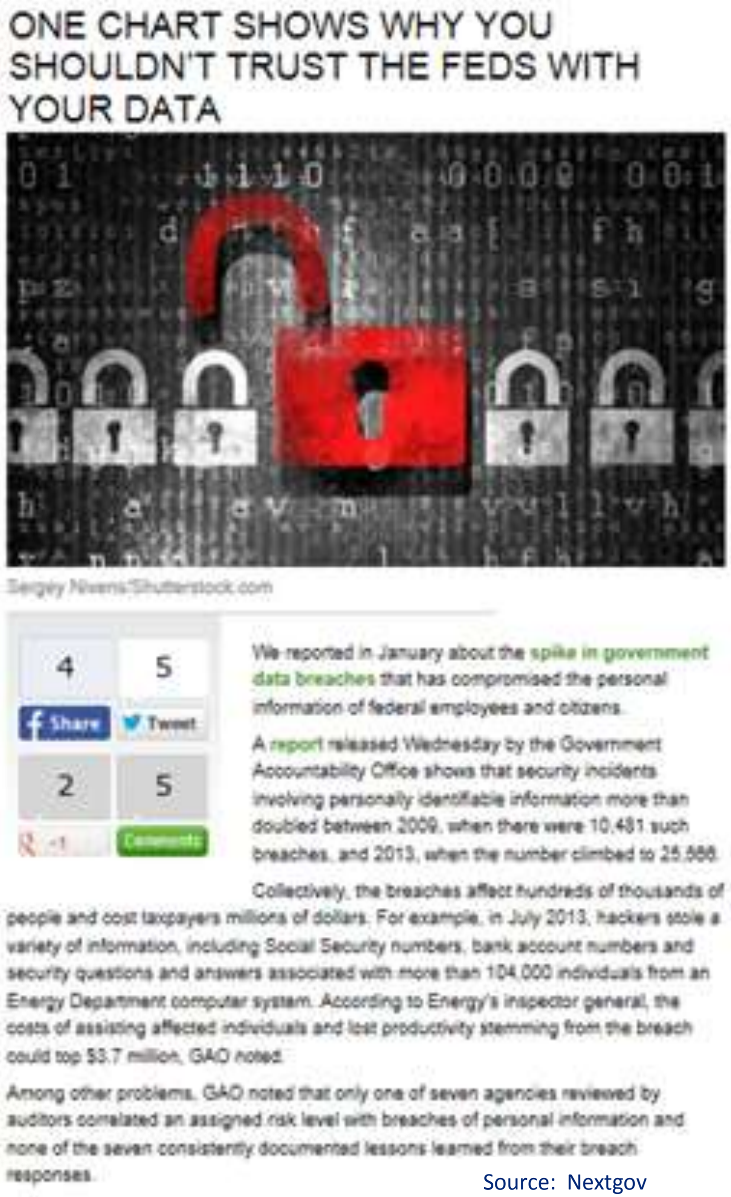
Sharing personal data is really good…

…with the right person.

But after 21 years, we still can’t solve this.

"On the Internet, nobody knows you're a dog."

And now we've got this happening.



ONE CHART SHOWS WHY YOU SHOULDN'T TRUST THE FEDS WITH YOUR DATA

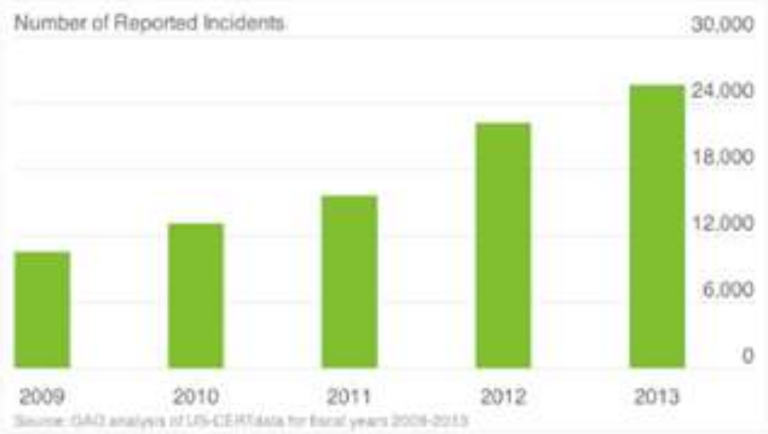
Sergey Nivens/Shutterstock.com

We reported in January about the spike in government data breaches that has compromised the personal information of federal employees and citizens.

A report released Wednesday by the Government Accountability Office shows that security incidents involving personally identifiable information more than doubled between 2009, when there were 10,481 such breaches, and 2013, when the number climbed to 25,566.

Collectively, the breaches affect hundreds of thousands of people and cost taxpayers millions of dollars. For example, in July 2013, hackers stole a variety of information, including Social Security numbers, bank account numbers and security questions and answers associated with more than 104,000 individuals from an Energy Department computer system. According to Energy's inspector general, the costs of assisting affected individuals and lost productivity stemming from the breach could top $3.7 million, GAO noted.

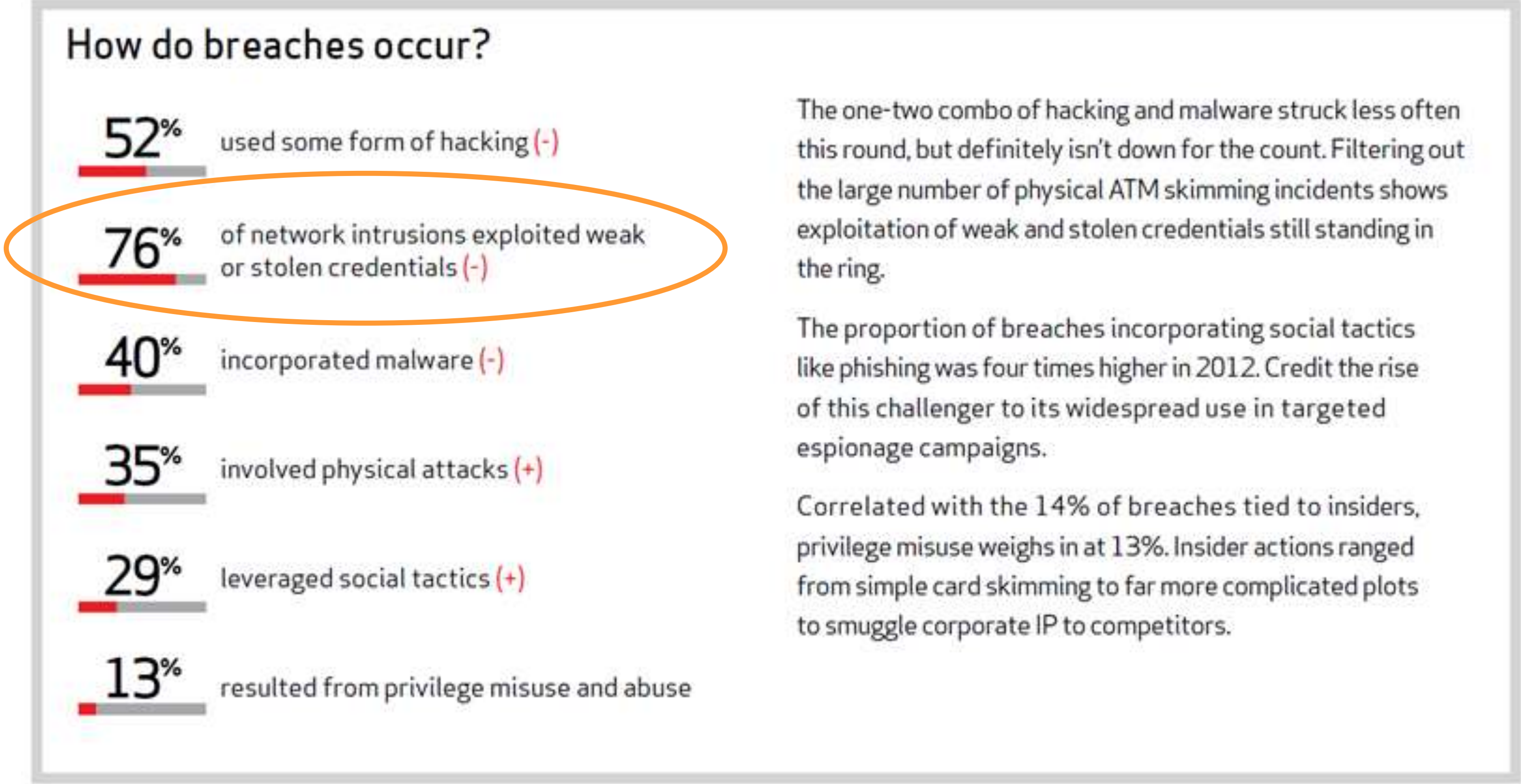
Among other problems, GAO noted that only one of seven agencies reviewed by auditors correlated an assigned risk level with breaches of personal information and none of the seven consistently documented lessons learned from their breach responses.



Source: GAO analysis of US-CERT data for fiscal years 2009-2013

Source: Nextgov

Securing personal data with just a password is a bad idea.



How do breaches occur?

52% used some form of hacking (-)

76% of network intrusions exploited weak or stolen credentials (-)

40% incorporated malware (-)

35% involved physical attacks (+)

29% leveraged social tactics (+)

13% resulted from privilege misuse and abuse

The one-two combo of hacking and malware struck less often this round, but definitely isn't down for the count. Filtering out the large number of physical ATM skimming incidents shows exploitation of weak and stolen credentials still standing in the ring.

The proportion of breaches incorporating social tactics like phishing was four times higher in 2012. Credit the rise of this challenger to its widespread use in targeted espionage campaigns.

Correlated with the 14% of breaches tied to insiders, privilege misuse weighs in at 13%. Insider actions ranged from simple card skimming to far more complicated plots to smuggle corporate IP to competitors.

Source: 2013 Data Breach Investigations Report, Verizon and US Secret Service

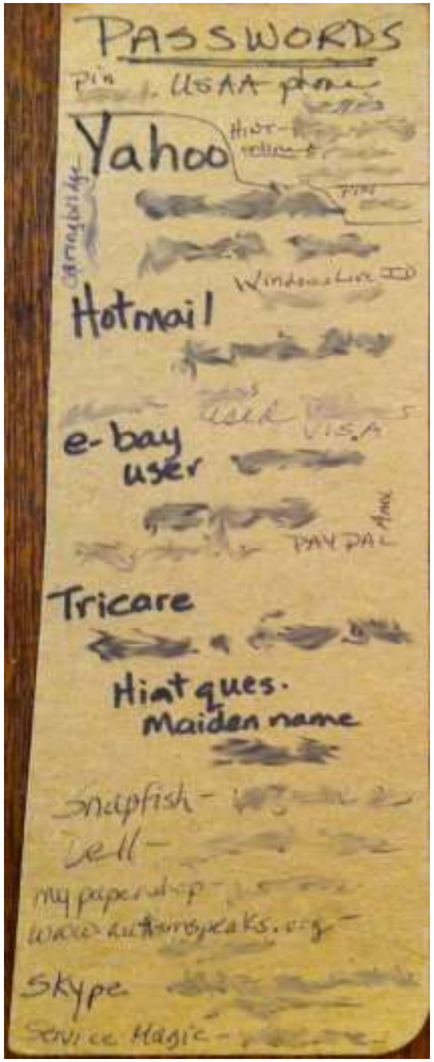
Agencies and apps can try to roll their own identity solutions.

But they probably can’t afford to do so.

And, we know the burdens of account creation heavily discourage user adoption.

- 75% of customers will avoid creating new accounts.
- 54% leave the site or do not return when asked to create a new password
- 45% of consumers will abandon a site rather than attempt to reset their passwords or answer security questions
- 38% of consumers would rather scrub their toilet than create a new password

When citizens already manage this:



PASSWORDS

Pin [redacted] USAA phone [redacted]

Yahoo Hint- [redacted]

PIN [redacted]

[redacted]

Cambridge

Windows Live ID [redacted]

Hotmail [redacted]

[redacted] user [redacted] VISA

e-bay user [redacted]

[redacted] PAY PAL Amx

Tricare [redacted]

Hint ques.
Maiden name [redacted]

Snapfish - [redacted]

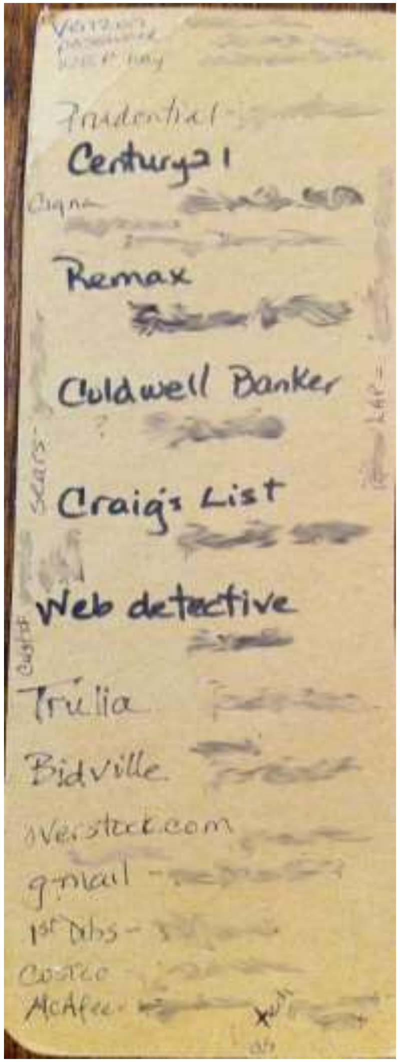
Dell - [redacted]

my paperdrop - [redacted]

www.autismspeaks.org - [redacted]

Skype [redacted]

Service Magic - [redacted]



Verizon password user ID [redacted]

Prudential - [redacted]

Century21

Cigna [redacted]

Remax [redacted]

Culdwell Banker [redacted]

Sears

Craig's List [redacted]

Web detective [redacted]

Trulia [redacted]

Bidville [redacted]

Overstock.com [redacted]

g-mail - [redacted]

1st Dibs - [redacted]

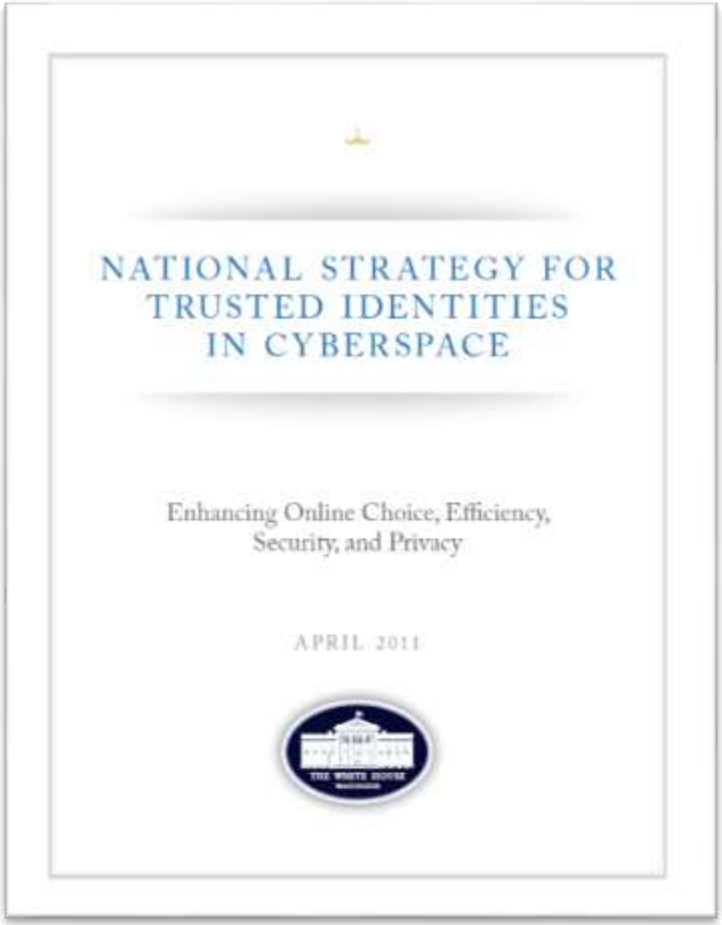
Costco - [redacted]

McAfee - [redacted]

They aren't eager to add another.

Citizens should be able to use a single, secure, convenient, privacy-enhancing credential across multiple sites – public and private – in lieu of passwords.

The President agrees.



NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

Enhancing Online Choice, Efficiency, Security, and Privacy

APRIL 2011

NSTIC calls for an **Identity Ecosystem**, "an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities."

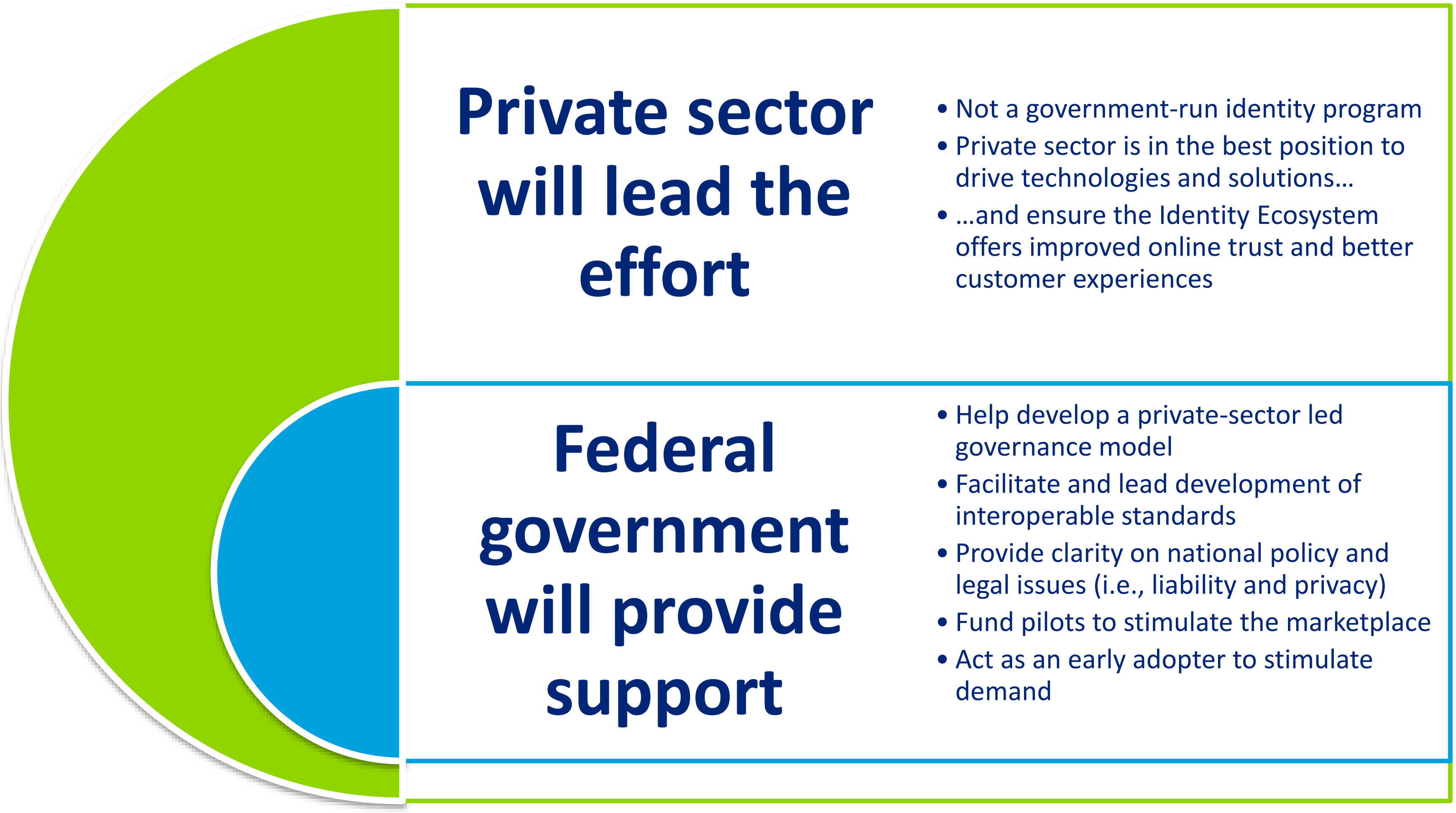
Guiding Principles

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use

Who else is at the table?

- Salesforce
- PayPal
- Verizon
- Fidelity
- Citigroup
- Mass Mutual
- IBM
- Visa
- Bank of America
- AARP
- EFF
- ACLU
- Microsoft
- Oracle
- 3M
- CA
- Symantec
- Lexis Nexis
- Experian
- Neiman Marcus
- NBC Universal
- Aetna
- United Health
- Kaiser Permanente
- Intel
- ADP
- MIT

What does NSTIC call for?



Private sector will lead the effort

- Not a government-run identity program
- Private sector is in the best position to drive technologies and solutions…
- …and ensure the Identity Ecosystem offers improved online trust and better customer experiences

Federal government will provide support

- Help develop a private-sector led governance model
- Facilitate and lead development of interoperable standards
- Provide clarity on national policy and legal issues (i.e., liability and privacy)
- Fund pilots to stimulate the marketplace
- Act as an early adopter to stimulate demand

Key Implementation Steps

Convene the Private Sector

- August 2012: Launched privately-led **Identity Ecosystem Steering Group (IDESG).** Funded by NIST grant, IDESG tasked with crafting standards and policies for the Identity Ecosystem Framework http://www.idecosystem.org/
- October 2013: IDESG incorporates as 501(c)3, prepares to raise private funds

Fund Innovative Pilots to Advance the Ecosystem

- Three rounds of pilot grants in 2012 and 2013; **11 pilots now active**
- Solicitations took a challenge-based approach focused on addressing barriers the marketplace has not yet overcome

Government as an early adopter to stimulate demand

- Ensure government-wide alignment with the Federal Identity, Credential, and Access Management (FICAM) Roadmap
- White House effort to create a **Federal Cloud Credential Exchange** (FCCX)
- August 2013: **USPS** awards FCCX contract

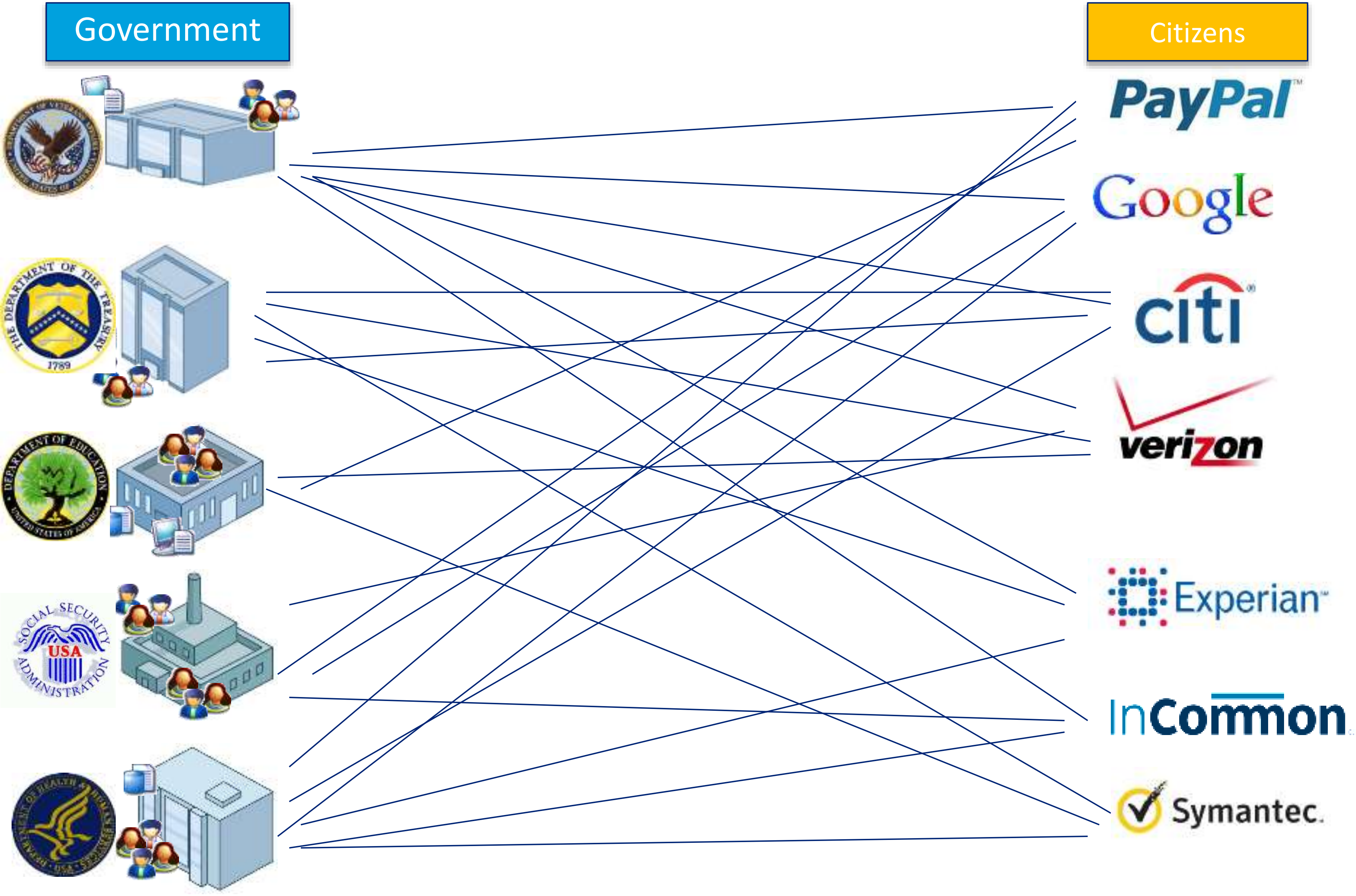
Agencies need a common solution that:

1. Tells each app:
   - ✓ "Is this the person really Johnny X?" (authentication)
   - ✓ "Which Johnny X of the 15 in my system is he?" (via validated attributes)
2. Provides an "easy button" on privacy and security
3. Ensures interoperability of these identity services across apps – both at a technical and policy level – so that a citizen can use the service across USG
4. Aggregates demand across government for these services – thus delivering discount pricing

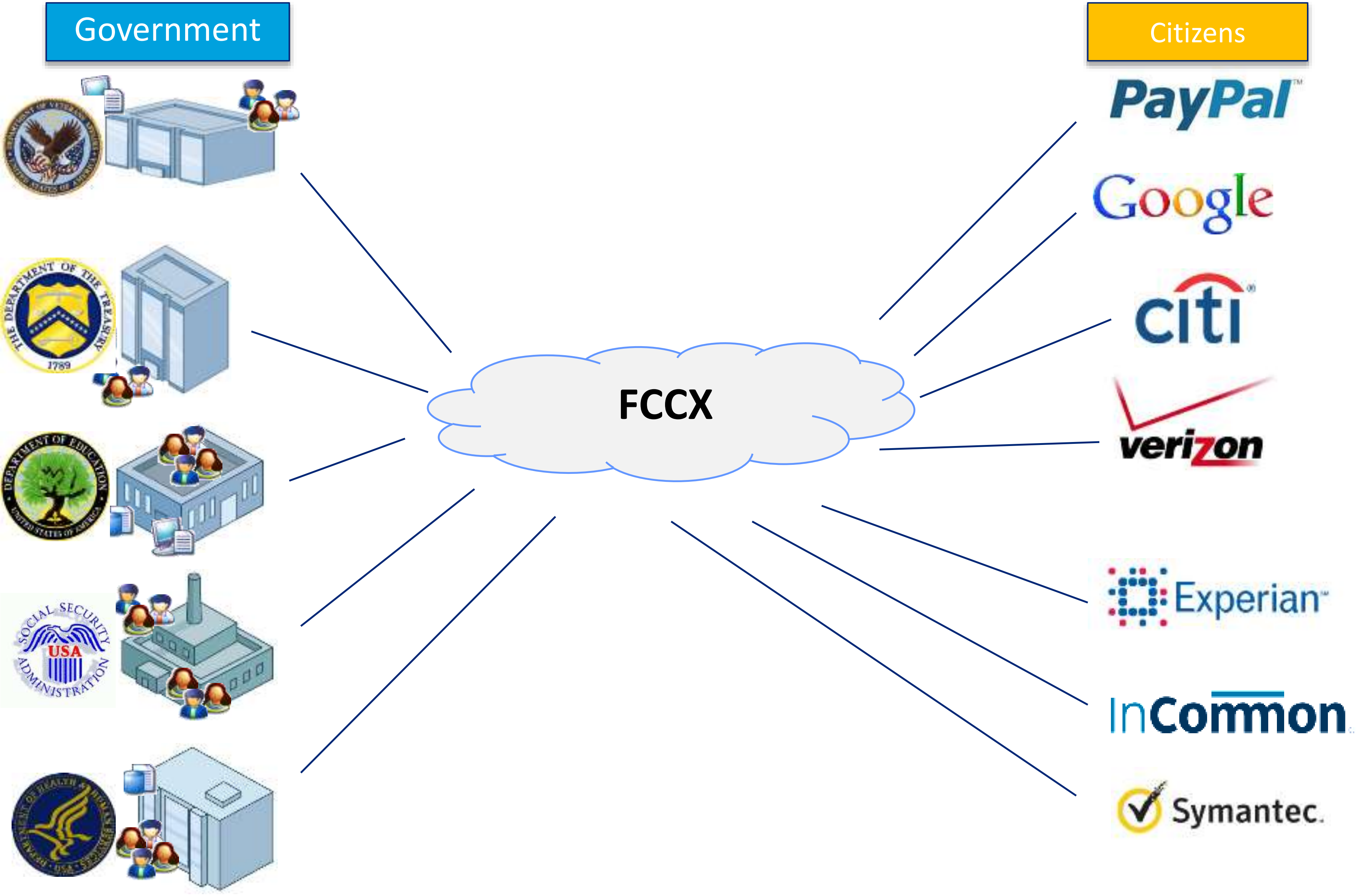
Thus…

The Federal Cloud Credential Exchange (FCCX)

Current Agency Environment



A better way


Government
Citizens
FCCX
PayPal
Google
citi
verizon
Experian
InCommon
Symantec.

FCCX is on track for fall expansion

- Production ready for LOA 1 and 4 by end of July (Google, Yahoo, PayPal, ID.me and PIV/CAC)

- Production ready for LOA 2 and 3 by end of summer (anticipate awarding at least 3 contracts to LOA2/3 commercial IDPs for USG-wide use)

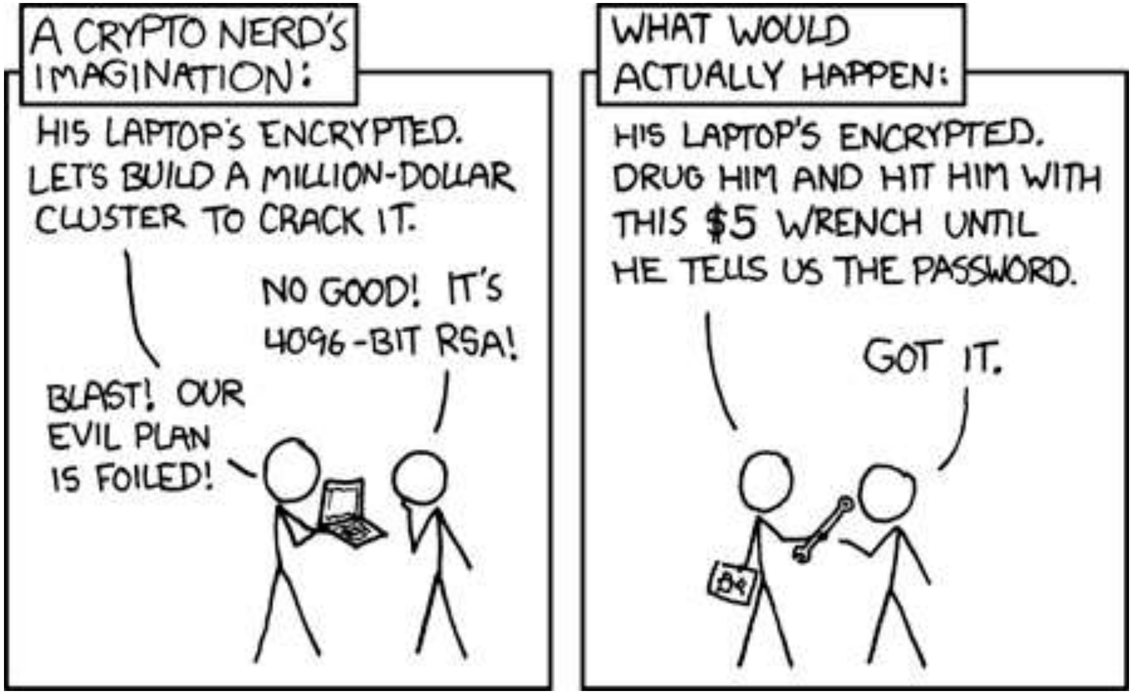
- VA/USDA/NIST launching apps this summer

- FCCX will be able to provide validated attributes with a SAML assertion to facilitate identity correlation/resolution activities at the Agency level:
    - ✓First, Last Name
    - ✓DOB
    - ✓SSN
    - ✓Address
    - ✓Email

Privacy is at the heart of FCCX

- Designed specifically to ensure that privacy requirements of anonymity, unlinkability and unobservability are built in from the start
- FCCX employs a “double blind” architecture – to prevent tracking of credential use among identity providers and relying parties.
- In simple terms, this means that private organizations that issue citizens credentials – and the agencies that accept them – will have no way to track where citizens use them.

It’s not all about security


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Source: *xkcd*

Usability

Liability

Privacy

Business Models

Interoperability

Questions?

Jeremy Grant

jgrant@nist.gov

202.482.3050